RECEIVED
CENTRAL FAX CENTER
JUL 2 6 2007

AMENDMENTS

In the Abstract:

Please replace the Abstract with the following Abstract:

A system and method for detecting and responding to device tampering in an Energy Management ("EM") ~~EM~~ device is disclosed. The EM device is provided with mechanisms to detect and indicate unauthorized tampering with the device. Further, in response to detected unauthorized tampering, the device may take actions to protect the integrity of data generated by the device as well as protect any confidential data stored within the device. Such actions may include preventing further device operation, generating warnings to the device owner/user, marking subsequently generated data as suspect, destroying stored confidential data, etc.

In the Specification:

Please replace the paragraph [0008] with the following paragraph [0008]:

[0008] One or more EM components may be coupled together in arbitrary configurations to form EM networks.

Please replace the paragraph [0071] with the following paragraph [0071]:

[0071] One way of reducing unauthorized access to EM Component 200 is for EM Component 200 to accept connections or packets only from pre-authorized addresses, where the address may be a phone number, IP address, MAC address, or other method for uniquely addressing a component. This is known as address blocking. Address blocking ensures that the user or server connecting to EM Component 200 is making contact from a pre-authorized location, which provides increased security against malicious attacks and may improve EM Component 200 performance during periods when it is targeted with traffic from unauthorized addresses, allowing EM Component 200 to continue functioning despite the attempted attack.

Blocking based on source address is far quicker than using Public Key Infrastructure ("PKI") ~~PKI~~ on every request, which is expensive processor-time-wise. Address Blocking is particularly relevant in the case where EM Component 200 is an EM device, as there are typically a limited number of remote, authorized connection locations. Address blocking also provides obscurity as it is harder for an antagonist to find a vulnerability to attack.

No new matter has been added.